What is ACT

ACT (Action against Cyber Theft) is a consumer awareness series by Suvarnayug Bank. With this series, the bank aims to promote steps that the consumer can take to avoid being a victim of cyber thefts. The intent is to encourage consumers to inculcate the practice of responsible banking.

With the growing internet penetration and associated technology, consumers are constantly under risk of the evolving nature of cyber crime; in this scenario, it is imperative that the consumers are educated and aware. ACT is a sustained, long term commitment to spread awareness among consumers and help minimize the risk of cyber theft.

As a force for good, Suvarnayug Bank aims to positively impact communities in which they operate and play the role of a catalyst in solving Asia's social challenges. In India, cyber thefts continue to remain a challenge for the consumers. This series will reach out to consumers at multiple touch points - television, print, radio, outdoor, theatres, on-ground activities and digital channels – to inform about cyber thefts. ACT aims to provide useful resources and information at one click.

Resources

Blogs

4 Important Steps That All Cyber Crime Victims Must Take

There has been a 350% surge in cyber crime cases registered in India*. From crude phishing emails to sophisticated malware attacks, the thefts are designed to steal private data or disrupt access to your systems

Factors like high-speed internet connectivity, increase in smartphones usage, and lack of awareness about Internet security often play a role in consumers falling prey to cyber criminals.

While it is advisable to be safe and secure, it is equally important to know what to do when you become a victim of cyber crime.

Here are some ACTions you should take to minimise the risk.

1. Disconnect and Detach

In case of an ongoing attack on your computer or IT infrastructure, your first step should be to disconnect the device from the Internet as this is the most effective way to prevent further loss of data

In case of cyber bullying or cyber stalking, one should simply step away from the screen before proceeding to initiate legal action.

In the event of a successful phishing attack where you are conned into revealing private and confidential information, you should immediately initiate steps like:

- Freeze your bank accounts and credit cards
- Alter your Internet and mobile banking passwords

2. Take Legal Action

Do not ignore and delay the process, initiate legal action even as you are trying to minimise the negative consequences of the cyber crime. Contact your local Cyber Crime Investigation Cell to file a written complaint against the cyber criminals. Provide detailed information about:

- Nature of the crime
- Extent of damage
- Relevant documents, data, and other information relevant to the compliant

Never make the mistake of presuming that cyber criminals cannot be caught. Provisions under the Information Technology Act and the Indian Penal Code define cyber crime as a punishable offence. Complaint against a crime committed in Delhi can be filed even in Mumbai. Hence, don't delay filing the complaint because the cyber crime occurred when you were out of town.

3. Inform your Contacts

Theft of your virtual identity can be misused by the cyber criminals to steal information and data from all your online contacts. Use social media to spread word about the incident. This simple step will minimise risk of your identity being misused to commit further crimes, and will ensure better awareness about cyber crime amongst your friends and relatives.

4. Take Preventive Steps for the Future

Install licensed antivirus software, use a strong password with a combination alpha numeric characters and never disclose your banking details to anyone.

While cyber thefts continue to remain a challenge and no one is immune to it, however the right ACTion at the right time will definitely help reduce the damage.

*Sources –

http://www.business-standard.com/article/current-affairs/indian-cyber-crime-soars-350-in-3-years-115011900329_1.html

http://www.helplinelaw.com/employment-criminal-and-labour/CCII/cyber-crimes-in-india.html

Effective Cyber Security Practices - 5 Benefits for Individuals and Organizations

A century ago, a suggestion that people all over the world will interact and exchange information irrespective of physical and geographical distances would have been ridiculed as mere fantasy. Today, the cyber world has transformed our lives.

However, the technology that allows you to communicate with a friend on the other side of the world can also be used for con you into disclosing private information online. While solutions like Dropbox facilitate real-time sharing of data, hackers can exploit 24x7-connectivity to steal private data stored on your unprotected computer.

A 2014 report by Center for Strategic and International Studies and McAfee, a fully-owned subsidiary of Intel Corporation indicates that cyber crime is causing the global economy to lose more than $400 billion every year. This data underlines the importance of focusing cyber security. Integrating safe practices in your online lifestyle can help you enjoy numerous benefits and advantages.

1. Financial Savings

In case of an ongoing attack on your computer or IT infrastructure, your first step should be to disconnect the device from the Internet as this is the most effective way to prevent further loss of data

Identity theft can allow a stranger to clean out your bank account. Submitting credit card data to unreliable sites can lead to significant liabilities. Firms that ignore online safety may end up being forced to allocate a lot of resources towards remedial and preventive measures. Recognizing the importance of online safety will help you enjoy the twin benefits of preventing theft and avoidance of unnecessary expenses on the remedial measures.

2. Peace of Mind

Accessing the Internet without an antivirus program or opting for simple and easy-to-crack passwords is the virtual equivalent of going on a vacation without locking your front door. Your safety will become a matter of luck and chance. Following effective cyber security rules and practices guarantees peace of mind. Simple steps like changing passwords frequently, paying for a quality antivirus program, and learning more about the potential risks of disclosing information to hackers and phishers will guarantee peace of mind.

3. Business Goodwill and Credibility

For a commercial organization, cyber crime can lead to significant loss of goodwill and credibility. With cyber crime becoming a global phenomenon, absence of sound security policies will reflect poorly on your goodwill and credibility in the global market. Any organization

seeking steady and sustainable growth cannot achieve its goals if it fails to protect its customers' data.

Creating security-consciousness amongst its employees and investing in robust security technologies will avoid instances loss of data due to hacking, phishing, or inadvertent leakage of information. An organization that fails to maintain cyber safety will quickly lose the confidence of its customer, and may not survive for long in today's competitive environment.

4. Strategic Benefit

Cybercrime is often described as a tax on innovation. A victim of cybercrime will be hesitant to explore and rely on new technologies. We are rapidly moving towards a world where Internet of Things will allow automatic communication between machines, and big data analytics will create safer, better, and a more productive life. Without cyber security, you may end up too scared to enjoy the strategic benefits of new beneficial technologies.

5. Foundation for the Future

Paying attention to cyber security is the most effective way to help the next generation understand the importance of virtual safety. Today, youngsters are at risk of numerous cyber threats ranging from hackers trying to encourage inadvertent disclosure of private information to individuals resorting to cyber bullying, harassment, and social embarrassment. A proactive approach towards cyber security will help the next generation imbibe lessons that will help them deal with such challenges in a confident and effective manner.

Conclusion

Cyber security involves something more than mere passive compliance with pre-determined safe practices. Cybercrime is evolving and the best way to maintain cyber security is to adopt a proactive approach towards virtual security at all times. Effective cyber security offers financial, social, practical, and strategic benefits in the present as well as in the future.

Important Precautions to Take to Enjoy a Safe Online Shopping Experience

Today, online shopping has become the preferred option for purchasing different products and services. Ecommerce sites allow you to compare numerous options from the comforts of your home or office. Further, buying online is a lot cheaper than buying from brick-and-mortar stores. However, online shopping will be fun and profitable only if cyber safety is given importance. One must keep the following precautions in mind to enjoy a risk-free online shopping experience.

Prefer Sites That Use Data Encryption

The presence of 'https' in the address bar indicates that the ecommerce site uses data encryption, which means no third-party can access or manipulate the information being transferred from your device and the e-shopping website. Unless the data is decrypted, the information transmitted will come across as meaningless letters and numbers. Data encryption is a must when transmitting details of your credit card, debit card, or bank accounts online.

Access the Site through Your Browser Address Bar

A well-disguised spam email promising great discounts may lure buyers to fake versions of popular ecommerce websites. One must avoid blindly relying on email newsletter links. Instead, type the address in the address bar of the browser to minimize risk of submitting financial information to a fraud website.

Research about New Sites on Social Media

Use social media to learn more about new online shopping sites before proceeding to buy from such sites. A quick visit to YouTube can help you view the site's video adverts, while the Facebook profile will help you assess the authenticity of the site. Further, seek feedback from your social contacts to ensure the site offers an authentic online shopping experience.

Consider Using One-Use Virtual Cards

Instead of submitting your credit card or debit card details to online shopping sites, consider using e-wallets or one-use virtual cards to minimize adverse consequences of theft or leakage of private data. Avoid saving your financial details online. Spending a few extra minutes submitting the credit card details can prove very beneficial in the long run.

Don't Trust Online Shopping Apps Blindly

A mobile app that allows online shopping from a mobile device or tablet can be a very convenient option. However, one must make sure the app is completely secure before using it. Research the app's security features before proceeding ahead. Pose queries to the online shopping site and consider their answers before shopping through the app. If unsatisfied, prefer using the web browser in your mobile device for online shopping.

Track Official Address of the Shopping Website

Make it a point to note the site's corporate address along with all contact details before placing the order. This will help you take further action in the unlikely event you are dissatisfied with services of the unprofessional ecommerce site.

Avoid Public Wireless Networks

Prefer shopping online from your home Internet network. If shopping through a mobile device, prefer using the data network of your mobile service provider over public wireless networks. Public WiFi hotspots allow third parties to access data transmitted by all connected devices. Minimize online shopping risks by transacting with encrypted sites over safe private networks.

Updated Antivirus Program

Don't shop online without installing an up-to-date antivirus program or app on your computer, laptop, smartphone, or tablet.

Conclusion

One can never be too cautious when conducting financial transactions over the Internet. Following basic cyber security rules will ensure the online shopping experience is a zero- risk affair. Further, have a conservative and common-sense approach towards online deals and offers from unknown sites that sound too good to be true. It is better to stick to reputed sites offering quality products at affordable prices when shopping online.

3 smart tips to safeguard your Smartphone

The Smartphone Users Worldwide 2012 – 2017 report by eMarketer has indicated that a by the year 2018 a third of the world's population will comprise smartphone users. The report also predicts that more than half of all conventional mobile phone users would have switched loyalties to smartphones by 2018.

Based on the current rate, India is set to become the second-largest base of smartphone users, more than 200 million, by 2016. Further, the report has indicated that more than nine out of ten Internet users shall access the web through their mobiles phones by 2017.

As smartphone Internet usage becomes more common, the number of people at risk from online security threats will also increase. Unlike a desktop or laptops, smartphone users face a larger number of security risks as security of the device is not even as secure as your traditional computer security, this must be effectively countered to enjoy a safe and risk-free smartphone experience.

Here is an overview of different types of security apps available for smartphones along with popular apps available in each category.

Anti-Virus Apps

Even reliable mobile OS like Android and Apple can have security loopholes that may allow malicious elements to gain access to private information and sensitive data like calendars, emails, contact information and passwords in your smartphone. The simplest and most effective way to safeguard your data is to install an anti-virus app on your device.

Apps like avast! SecureLine VPN and 360 Mobile Security provide real-time protection from online risks along with conventional features like firewalls, anti-spyware tools, usage history clearing, and virus scans. These apps also allow you to filter text messages and calls, and enable users to 'trust' certain SIM cards, which allows them to execute remote changes even if the phone is in the hands of a third person.

With millions of apps available online, and there being no effective mechanism to assess the safety and reliability of the apps, a functional antivirus app, free or paid, will provide effective protection for your smart device.

Theft Protection

While smartphones are as functional and useful as laptops, these mobile devices are a lot easier to steal and almost impossible to trace. You can improve your chances of recovering a lost or stole smartphone by installing apps that allow you to track the phone's location through its inbuilt GPS mechanism.

Apart from tracking the device, these apps also allow you to backup the phone's data online before wiping it clean. This feature ensures your private data remains confidential even if you are unable to recover the phone.

Apple was the first to install a kill switch in its iPhones in 2013, which allows owners to remotely 'kill' or shutdown a stolen phone. If your phone does not have a kill switch, then you can opt for apps like Lookout, Find My iPhone, or Android Device Manager to wipe the phone if remote tracking fails.

Password Management

With banks and other service providers offering smartphone apps, users are required to keep track of multiple passwords for email accounts, phone accounts, and a large number of apps. Instead of storing your passwords as a text message in your phone, you can use apps like LastPass that lets you keep a record of all your passwords without any security risks.

Apps like LastPass require you to remember just the app's password, which, if entered correctly, will help you view all other passwords. This app lets you track your passwords over multiple devices, which is a useful option for this using multiple tablets and smartphones.

With hackers relying on adware apps, Trojan SMS messages, and backdoor programs to gain unauthorized access to smartphones, it is important to combine sensible usage practices with quality security-related apps to secure your smartphone and its data. Be smart, be safe and #ACTNow.

Is Your Organization's IT Security at Risk?

According to the 2013 Norton Report which covered over 13,000 respondents from 24 countries, almost half the respondents used their personal computing devices for work-related activities. Further, close to 50% of the respondents admitted that they were using their computers and smartphones without implementing safety measures like use of strong passwords and installation of security softwares. This has made them attractive targets/sitting ducks for attackers.

The Norton Report indicated that the average direct cost of cybercrime works out to around $300 per victim. Considering indirect costs like liability claims and other intangible negative consequences, a careless employee who ignores basic cyber safety rules and precautions can put the organisation's solvency and market credibility at risk. Make sure you don't commit these online safety mistakes at your workplace.

1. Reusing Passwords

A strong password is the most effective way to safeguard your office IT assets including computers, servers, and networks from unauthorized access. The policy requiring employees to change their passwords at regular intervals is rendered futile by employees who simply use to reuse their old passwords.

Or, they have a set of passwords stored in the office computer for easy access. Such an approach mitigates the effectiveness of using passwords to protect your IT assets. Don't reuse passwords, avoid having a list of stock passwords to be used one after the other, and avoid opting for passwords that can be easily guessed.

2. Sharing Passwords

The password helps the organization create and implement hierarchy of access to IT assets amongst employees. It also helps track usage of networks, assets, and devices amongst different users. Sharing passwords makes it impossible for the firm to know which employee is using which asset within the network. Further, sharing increases the risk of private and confidential information leaking out to unauthorized persons.

Entering your passwords on your own is unlikely to require more than 10-15 seconds of extra effort as compared to sharing the password. Keep your passwords private and make sure you change it in the event you are compelled to share it with a colleague.

3. Leaving IT Assets Unattended

Employees often err in presuming that only a major mistake or error will result in cyber safety issues. Even something as ordinary as leaving the desk without logging out of your workstation or enterprise-level cloud can pose a security risk. This small mistake can allow a visitor gain access to the organization's network. From installation of remote tracking software to

unauthorized copying of data — leaving IT assets unlocked and unattended can render all other workplace safety measures ineffective.

4. Connecting Personal Devices to the Organization's Network

Apart from wasting precious resources of the firm for private use, such a mistake can allow hackers to gain access to the secure network through your unprotected or poorly-secured private device. Firms with BYOD (Bring Your Own Device) policies require employees to follow stringent norms.

Consider installing online security solutions offered by reputed brands like McAfee, Norton, Quick Heal, or Kaspersky. Anti-virus and anti-malware programs offer real-time protection from Trojans, viruses, and malwares. The firewall will ensure your device does not serve as conduit for hackers seeking access to your office network. Ignoring the norms or connecting personal devices when the firm does not have a BYOD policy can have negative effect on workplace security.

5. Copying Work Data to Personal Devices

This is a significant risk that can magnify the consequences of end-user carelessness. A University of Alabama study revealed that 80% of companies view employee carelessness as the biggest IT security risk. Using unencrypted flash drives to copy work data on personal devices or storing information on laptops can prove to be a major security risk. Loss of device or unauthorized access is enough for the firm's private data to be leaked online.

Devastating workplace safety breaches occur primarily due to numerous seemingly-minor mistakes, errors, and policy violations amongst employees. No precaution should be considered insignificant when online safety is at risk. Even something as minor as placing a sticky note on unused webcams can prove beneficial in the long run.

Reliable workplace IT security depends on awareness and respect for safety rules amongst employees, rigid obedience of rules, and a proactive approach towards protecting the firm's IT infrastructure from the latest threats.

An Introduction to the World of Ransomware

Ransomware, as the name suggests, is a computer malware that prevents users from accessing their computer systems unless they pay a ransom to the cybercriminals. Unlike other viruses where users have to spend money to remove adware and other malware installed in the system, ransomware requires the user to literally buy back their access to their own computers. It is the cyber version of blackmail where criminals force individuals to pay a ransom to recover their loved ones or precious belongings.

Evolution of Ransomware

According to TrendMicro, the earliest ransomware cases, which originated in Russia in 2005-06, created password-protected zip files of documents, spreadsheets, programs, and DLL files. The user was required to pay a ransom to obtain the password and regain control over his or her system.

By 2012, ransomware attacks had spread into Europe, Canada, and the USA. The attacks became more sophisticated as cybercriminals began using a wide range of websites to infect computers, and pretended to be law-enforcement agencies to scare affected users from going public about the attack.

In 2013, a new variant emerged that, apart from blocking access, encrypted the files of the system. This meant that users could no longer recover access by simply deleting the malware. The user would still have to pay ransom to decrypt the files. These variants are called CryptoLocker, a reference to the fact that the system's files are locked due to crypto-encryption.

Other variants include

- Malware that require steal bitcoins or require payment of ransom in bitcoins
- Attacks that focus on the inbuilt PowerShell feature in MS Windows 7 and above
- Instances where backup files are deleted to prevent the user from bypassing the encryption, and
- Attacks that block access to remote drives as well.

Impact of Ransomware Attacks

Unlike conventional virus and malware attacks, ransomware makes it impossible for the user to access his or her files until the problem is solved. For a business, the prospect of databases built over decades becoming inaccessible can affect the very existence of the business. Basic tasks like meeting deadlines, responding to mails, or updating internal spreadsheets will become impossible.

Apart from impact on productivity, ransomware attacks can affect the firm's or individual's finances as well. Ransomware: A Growing Menace, a report by Norton security experts, analyzed a specific attack covering 68,000 computers in a month with ransom demands ranging from $60 to $200. Experts found that payout resulted in a loss of $33,600 for 168 users. With

less than 3% of victims paying the ransom, the criminals could have made close to $400,000 in a single month. This analysis clearly reveals that ransomware attacks pose a very real threat to the finances and functioning of any individual or business depending on IT products and services as a part of their routine activities and operations.

Future of Ransomware

The Europol's 2014 Internet Organized Crime Threat Assessment has warned about ransomware attacks on medical devices like pacemakers, medical information systems in hospitals and devices, as well as attacks on Internet of Things.

With Internet connectivity becoming an integral part of our lives, a hacker situated thousands of miles away can hold all aspects of our lives at ransom through sophisticated ransomware attacks.

Protection from Ransomware

The best way to escape ransomware attacks is to focus on preventive action. The following steps can help individuals and businesses avoid becoming victims of a ransomware attack.

- Having an up-to-date antivirus program that offers traditional file-based security to detect and block ransomware files.
- Network-based security tools that track and block attempts by hackers to penetrate corporate and personal networks.
- Tools designed to detect files displaying ransomware-like behaviour in computers and on networks.
- Programs that offer reputation-based protection by warning surfers when visiting infected or unsafe websites.
- Standard security practices like avoiding downloads from random emails and tracking common social engineering techniques used by cybercriminals.

Finally, one can minimize negative impact of a successful ransomware attack by having network-independent backups to minimize risk of loss of access to the files.

Further, one can use recovery tools offered by reputed online security brands to recover control of infected systems.

Sources

https://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/ransomware-a-growing-menace.pdf

https://www.us-cert.gov/ncas/alerts/TA14-295A

http://www.trendmicro.com/vinfo/us/security/definition/ransomware

http://www.raps.org/Regulatory-Focus/News/2014/10/09/20535/Money-or-Your-Life-Report-Predicts-Ransomware-Affecting-Medical-Devices-in-Near-Future/

Protect Yourself from Phishing, Vishing, Smishing and Pharming

According to the 2014 Review by RSA, the security division of EMC Corporation, Indian Internet users are increasingly targets of phishing attacks on the Internet.

Such attacks have resulted in losses of $15 million for Indian surfers in just the first six months of the previous year. Rising computer and smartphone usage and broadband Internet penetration is putting India at risk of further increase in phishing attacks. It costs only $75 for hackers to send 500,000 phishing emails which means that one just cannot afford to underestimate this problem.

Read ahead for more information about phishing and its numerous variants along with measures that can help you protect yourself.

Phishing and its Variants

Just as fishing involves placing the bait in the water and waiting for the fish to bite, phishing is an attempt by cyber criminals to con computer users into disclosing private information like PAN details, bank account information, credit card details, and other personal information that can be used for identity thefts.

The crime begins with a generic email or chat message, which invariably contain messages like:

- Promise of foreign fund transfers
- Opportunity to interact with attractive man or women
- Warnings from authorities about problems in one's banking records

The email tries to convince the reader to click on a link, download a file, or reply with certain personal and financial details. If the reader complies, the criminal will use subsequent interactions to acquire more information and details.

Vishing

Vishing refers to voice-based phishing. Now that mobile banking has become very common, criminals pretending to represent banks, credit card service providers, tax authorities, or even utility companies use social engineering techniques to trick the victim into revealing private information.

Smishing

With smart phones allowing individuals to access bank accounts on the move, cyber criminals are using text messages with links to malicious sites or phone numbers that lead to official-sounding requests for your account details, PIN, and other personal information to perpetrate identity theft.

Pharming

Pharming involves the installation of a malicious software or code on the user's computer through emails and chat messages. The code leads you to malicious versions of your bank or credit card websites. A pharming victim ends up submitting online banking details to cyber criminals without even realizing it.

Protective Measures

Although tactics may vary depending on the medium, all crimes described above succeed primarily due to the carelessness, lack of awareness, and absence of caution on the part of the victim. The following measures can help you minimize the risk of becoming a victim of phishing and other cybercrimes:

- Don't disclose personal or financial information to strangers through email, chat messages, SMS, or telephone calls. The risk of offending a stranger is preferable to the risk of becoming a victim of identity theft.
- Down download files sent by strangers even if the message does not seem suspicious.
- Never reply to unsolicited requests from persons claiming to represent banks or tax authorities.
- Don't visit your bank's website through email links. Type the address in the browser's address bar.
- Make sure you are not visiting a fraudulent site by checking the site's identity information. All banking sites work with agencies like VeriSign that provide independent confirmation of the site's authenticity. Just click on the lock adjacent to the site's name in the address bar.
- Install a quality anti-virus and anti-malware program in your computer, laptop, tablet, and smartphone.

Links

http://www.emc.com/collateral/fraud-report/rsa-online-fraud-report-012014.pdf
http://india.emc.com/microsites/rsa/phishing/index.htm
http://securityresponse.symantec.com/en/uk/norton/clubsymantec/library/article.jsp?aid=cs_smishing_vishing

Online Banking Precautions You Cannot Ignore

Banking, with its rigid rules, detailed procedures, odious paperwork, and technical jargon, was always considered as something best left to our parents to worry about. While banking processes have not become simpler, improvements in technology have made it easier and more convenient to perform routine transactions.

However, we make the mistake of ignoring simple and basic measures and precautions that can help us avoid falling prey to cyber thefts. One does not have to be a computer genius to know that accessing online banking account through a computer infected with viruses, Trojans, keylogger programs, and malwares can result in theft of private and confidential banking information. Phishers and Vishers may use a combination of poor security and social engineering to steal your identity and all your money. But somehow do not take the necessary precautions.

Here are some precautions one must keep in mind when using online banking services or when using Internet payment systems involving your bank.

Use a Secure Computer

The importance of using a secure device with an updated antivirus and antimalware program cannot be over exaggerated. A secure computer will protect your private information even if you accidently allow cyber criminals to install a malicious code in your computer.

Real-time scanning and protection will resolve the problem before any significant damage takes place. Accessing your online bank account or making payments online on an unsecured computer will

Use Banking-Specific Safety Features

Computer-safety programs have started offering in-built banking-centric safety features like a virtual safety environment that provides continuous protection against phishing, key logger programs, and identity-theft attempts when you are accessing your banking account through your computer.

Use On-Site Security Features

Most banking sites allow you to enter your user id and password through on-site virtual keyboard instead of your computer's keyboard. This will help you minimize the risk of your login and password details being tracked or logged by malicious programs.

Verify Authenticity Of the Banking Site

Type the bank's address in your browser's address bar instead of using links received in emails and chat messages. This will ensure you don't submit private information to a fraudulent site. Further, verify the site's authenticity by ensuring that the site has been verified by an independent authentication service like VeriSign.

Use Multi-Step Authentication

Go beyond the conventional authentication process that requires the user to submit a transaction password to confirm the transaction. Instead, opt for multi-step authentication that involves entry of a One-Time Password sent by the bank to the registered phone number, or submission of a third password. This will ensure cyber criminals cannot access your account even if they steal your login details.

Ensure Data Transmission is Encrypted

The presence of 'https' in the address bar is proof that the data being transmitted between the server and your computer has been encrypted. This means the information you transmit can be read and understood only by the bank's server. Any third-party hacking into the transmission cannot decrypt and access the information.

Secure Account-Reset Data

Instead of the bank account details, phishers and vishers focus on data and information that can be used to reset your online banking account. Banks allow users to reset their login and transaction passwords by submitting additional information like PAN data, date of birth, and other personal details. Disclosing information like your mother's maiden name or your first car's license number can be as risky as disclosing your login or transaction password to a stranger.

It is not very difficult to protect your online banking account. You just need to use common-sense precautions, a secure computer, and the security features available on the site to keep your details safe.

What is Online Identity Theft and How do You Tackle It?

Section 66 of India's Information Technology Act defines identity theft as use of electronic signature, password or any other unique identification feature of a person for dishonest or fraudulent purposes.

Identity theft includes instances like:

- • Hacking into a person's mail account and sending an email in his or her name,
- • Stealing a credit card and using it at an outlet, or
- • Pretending to somebody else on a social media site for dishonest or fraudulent purposes

The Internet, with all its advantages and benefits, has made it easier for cyber criminals to steal identity and misuse the information. In the real world, a person in possession of your identity card cannot just walk into your office pretending to be you. In the virtual world, a person who knows your passwords or credit card information is, for all practical purposes, the owner of your identity. Online identity theft can take place in the following ways.

Social Media Tracking

Criminals are eschewing crude tactics like sifting through trash and are relying on sophisticated methods like identity theft through social media tracking. Social media profiles that are visible to all Internet surfers can be used by cyber criminals to collect details like birthdays, the identity and personal details of the individual's family members, mother's maiden name, their online banking service provider, and other such details.

Hackers often use this information to impersonate the individual on the Internet. Social media updates can be used by hackers to seek money for reasons like the wife's birthday or an emergency during a foreign vacation. Recipients may find it difficult to suspect mails filled with accurate references to personal details.

Medical Identity Theft

Instead of hacking individual computers, cyber criminals are targeting data stored in corporate organizations, hospitals, and even online gaming sites. A report released by Ponemon Institute on behalf of the Medical Identity Fraud Alliance (MIFA) reveals a 20% Y-o-Y increase in medical identity theft in the USA in 2014. 65% of the victims spent around $13,500 to resolve the theft and the misuse of their private medical information.

Copyright Infringement

All posts, updates, images, videos, and logos associated with your business represent your firm's intellectual property. In a globalised market where consumers rely on logos, images, and trademarks to distinguish brands, copyright theft can easily lead to theft of your identity.

Unlike other instances of identity theft, it may take a long time for you to realize that content over which you have copyright has been stolen and misused. The financial and reputational impact too may take place over a long time. The most effective way to tackle this problem is to track all your content and take firm and immediate action somebody attempts to steal your copyrighted content.

Phishing

This cybercrime involves use of social engineering techniques to either con the individual into disclosing his or her private and confidential information, or to extract information through download of malicious codes and programs into the individual's computer. Keyloggers, Trojans, and other viruses will track your transactions on the Internet, and extract details like online banking User IDs and passwords, credit card numbers, CVV details, and other private information through your online submissions.

Tackling Online Identity Theft

The 2014 release of Microsoft's Annual Computing Safer Index indicates that 20% of respondents from India had fallen prey to phishing attacks and suffered an average loss of Rs.7500 per person. The survey estimates that global loss from phishing and other forms of identity theft at around $5 billion. Further, the cost of repairing the financial and other damage is estimated at around $630 per transaction. To keep private information safe from such criminals, one must consider the following precautions:

- Carry out online transactions through a secured device with an up to date antivirus and anti-malware software application.
- Never disclose private information through mails, chat messages, telephone, SMS, or through IVR phone calls.
- Make sure your social media profile is not accessible to strangers. Be careful of what you share with others.
- Using virtual payment cards for online shopping transactions. When submitting your credit or debit card details, make sure the information is not stored online

The Internet is becoming the preferred medium of communication, commerce, and other transactions. It is advisable to learn more about safety risks like identity theft, and the various steps and strategies that one should take to prevent cyber crimes.

Is Your Child Cyber-Safe? Check Today; Be a Responsible Parent

It's the start of the summer vacations, a time of the year when your child has a lot of free time and stays glued to the devices either playing games or watching videos. With a third of India's population aged less than 14 years, online safety for children is an issue of paramount importance.

Unlike adults, children cannot understand the risks involved in sharing the family's daily routine, their holiday plans, time when there are no adults at home, and other such details with a complete stranger on the Internet. From phishers and hackers to pedophiles, there are numerous risks that kids must be safeguarded from on the Internet. That is why parents need to be more proactive in making sure children are secure online.

Online child safety is a process that will require different tactics and strategies depending on the age and maturity of the children. Denying unmonitored access is the safest way to protect young children from online risks. Combining supervised Internet surfing with tools like parental controls and filters is an effective strategy for youngsters.

Demanding complete obedience may not work well with adolescents and teenagers. The best way to protect them is to combine education and awareness with monitoring and self-discipline. A responsible parent can rely on the following strategies to secure online child safety.

Establish Ground Rules

Unrestricted and uncontrolled Internet access is a shortcut to disaster. It is very important to establish clear and firm ground rules related to Internet access for children. Some useful rules for youngsters include:

- • No unsupervised Internet surfing
- • No access to chat rooms or social forums
- • No upload of photos or other posts on social media sites without permission
- • Clear timetable for Internet access

Monitor Online Habits

It is important to monitor your child's online surfing habits. Every quality antivirus and antimalware program includes parental control features and content filters to protect children from online risks. You can combine such programs with tools like NetNanny that are designed specifically to monitor your child's activities on the computer and on the Internet.

Inculcate Awareness

Ultimately, self-discipline and awareness about online risks are the best safeguards against online risks. Combine strict rules and regular monitoring with educating your child about cyber risks and its potential implications. Explain how seemingly-innocent details like future holiday plans and parents' work schedule can put your child at risk.

Use online resources to help your child understand how phishers and hackers target young children. Further, educate your child about cyber bullying and risks of accessing inappropriate content. Organize a group activity for your child and all his or her friends to ensure the learning and awareness about cyber safety can become a social and peer-based activity.

Encourage Children to Speak Up

While you should try your best to protect your kids from cyber risks, you should also encourage the child to speak up in the event they commit a mistake. Children may hide instances of identity theft, cyber bullying, or inappropriate interaction initiated by a stranger on the Internet out of fear of being punished.

Create an environment where the child can speak about such topics in a confident manner. This will help you take action against any unsafe cyber activity before it causes a lot of damage to your child.

The Internet is here to stay, and helping your child understand the importance of online safety will be a valuable lesson that will help him or her for a long time in the future. Combine technology and firm parenting with open communication to keep your child safe from online risks at all times.

Research

http://www.fosigrid.org/asia/india

FAQs

What is this site about?

ACT (Action against Cyber Thefts) is a site to raise awareness against cyber theft and to educate people about cyber security.

What kind of information will I find on this site?

You may find issues related to cybercrime.

- Cybercrime news
- Blogs
- Resources- Important links and information
- Contact us for queries
- Safety tips
-

How can ACT help me?

-
- ACT provides you with information on kinds of cyber crime. Visit Resources to find important links and safety tools. Visit our Blogs to know more about the topic in detail.

What is cybercrime?

Cybercrime is a crime which uses computer or the internet to carry out illegal or criminal activities. It is becoming a widespread epidemic not only across India but worldwide. Cyber crime takes many faces and is committed in diverse ways.

What information is required to lodge a complaint?

According to the cyber Crime Investigation Cell, here is the information that is required.

If you are a victim of hacking

Bring the following information:

- Server Logs
- Copy of defaced web page in soft copy as well as hard copy format, if your website is defaced
- If data is compromised on your server or computer or any other network equipment, soft copy of original data and soft copy of compromised data.

- Access control mechanism details i.e.- who had what kind of the access to the compromised system
- List of suspects – if the victim is having any suspicion on anyone.
- All relevant information leading to the answers to following questions

- What? (what is compromised)
- Who? (who might have compromised system)
- when?(when the system was compromised)
- why?(why the system might have been compromised)
- where?(where is the impact of attack-identifying the target system from the network)
- How many?(How many systems have been compromised by the attack)

If you are a victim of e-mail abuse, vulgar e-mail etc.

Bring the following information

- Extract the extended headers of offending e-mail.
- Bring soft copy as well hard copy of offending e-mail.
- Please do not delete the offending e-mail from your e-mail box.
- Please save the copy of offending e-mail on your computer's hard drive.

Why do we need to fight Cybercrime?

Fighting cybercrime is as important as fighting on-ground crime. It is a breach of one's personal space and privacy online. Such crimes may also threaten a nation's security and financial health. The crimes themselves are not necessarily new – such as theft, fraud, illegal sales, pornography – but they are evolving in line with the opportunities presented online and therefore are becoming widespread and damaging.

Where do I find a complaint centre?

Click here to Find nearest complaint centre

Cyber Crime Divisions

Mumbai

Cyber Crime Investigation,
Cell Office of Commissioner of Police office,
Annex -3Building, 1st floor,
Near Crawford Market, Mumbai- 400 001.

- : 022 - 22653714
- : cybercell.mumbai@mahapolice.gov.in
- : http://www.cybercellmumbai.gov.in/

Gujarat

Cyber Crime Investigation,
DIG, CID, Crime and Railways Fifth Floor Police Bhavan Sector 10, Gandhinagar 382009

- : 079-2325 0798
- : -
- : -

Hyderabad

Cyber Crime Investigation,
Crime Investigation Department, 3rd Floor, D.G.P. office Lakdikapool, Hyderabad – 500004

- : +91-40-2785 2040, 040-27854031
- : cidap@cidap.gov.in, info@cidap.gov.in
- : http://www.cidap.gov.in/contact/contact.aspx

Jammu

Cyber Crime Investigation,
SSP, Crime CPO Complex, Panjtirthi Jammu-180004

- : +91-191-257-8901
- : sspcrmjmu-jk@nic.in
- : -

Tamil Nadu

Cyber Crime Investigation,
A-Wing, III rd Floor, Rajaji Bhawan, Besant Nagar, Chennai-600090

- : 044-24461959
- : spcybercbcid.tnpol@nic.in
- : www.cbcid.tn.nic.in/contactus.php

Can I lodge my complaint on this site?

Unfortunately, this site only caters to information requirement. You can lodge your complaint by clicking through the links given: Important links

Cyber Crime Information

CAT -Cyber Appellate Tribunal (CAT)

In accordance with the provision contained under Section 48(1) of the IT Act 2000, the Cyber Regulations Appellate Tribunal (CRAT) has been established in October 2006. The Cyber Regulations Appellate Tribunal after the amendment of the IT Act in the year 2008 (which came into effect on 27.10.2009) is known as the Cyber Appellate Tribunal (CAT). As per the IT Act, any person aggrieved by an order made by the Controller of Certifying Authorities, or by an adjudicating officer under this Act may prefer an appeal before the Cyber Appellate Tribunal. This Tribunal is headed by a Chairperson who is appointed by the Central Government by notification as provided under Section 49 of the IT Act 2000.

Before the amendment of the IT Act in the year 2009, the Chairperson was known as the Presiding Officer. Provision has been made in the amended Act for the Tribunal to comprise a Chairperson and such number of other members as the Central Government may notify / appoint.

Read more here. http://catindia.gov.in/Default.aspx

ICERT- Indian Computer Emergency Response Team

CERT-In has been designated under Section 70B of Information Technology (Amendment) Act 2008 to serve as the national agency to perform the following functions in the area of cyber security:

- Collection, analysis and dissemination of information on cyber incidents
- Forecast and alerts of cyber security incidents
- Emergency measures for handling cyber security incidents
- Coordination of cyber incident response activities
- Issue guidelines, advisories, vulnerability notes and whitepapers relating to information security practices, procedures, prevention, response and reporting of cyber incidents

For more information click here: http://www.cert-in.org.in/

CAA- Controller of Certifying Authorities

Section 18 of the Information Technology Act, 2000 provides legal sanctity to digital signatures based on asymmetric cryptosystems at par with signed paper documents. The section 17 of the Act provides for the Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities. The Certifying Authorities issue digital signature certificates for electronic authentication of users.

The Controller of Certifying Authorities (CCA) has established the Root Certifying Authority of India (RCAI) under section 18(b) of the IT Act to digitally sign the public keys of Certifying Authorities (CA) in the country. The CCA certifies the public keys of CAs using its own private key, which enables users in the cyberspace to verify that a given certificate is issued by a licensed CA.

Find more details here: http://www.cca.gov.in/cca/

Can you mention some tips to prevent Cybercrimes?

Before it catches up to you, you should catch up with it. Here are a few tips to prevent cybercrime:

- Update passwords and login details
- Maintain latest softwares and updates to protect your PC.
- Be social media savvy- set your profiles to private.
- Secure mobile devices using mobile protection software or having a screen lock.
- Protect your Data by using encryption methods and back-ups
- Be aware of what you do while using public Wi-Fi Hotspots.
- Protect your e-identity and be wary of giving out personal information.
- If you are a victim, get help as soon as possible.

What are the most common cybercrimes?

Here is a list of most common cyber criminal activities:

- Phishing/ Extortion
- Blackmail
- Hacking or accessing stored information without permission
- Fraud over the internet
- Electronic harassment
- Child pornography or prostitution
- Copyright infringement
- Malware or software errors